Remarks

This responds to the final Office action mailed April 5, 2007 ("the Action"). Reconsideration of the application is respectfully requested in view of the following remarks. Claims 1-20 are pending in the application. No claims have been allowed. No claims are amended. Claims 1, 2, and 13 are independent.

Cited Art

U.S. Patent No. 6,263,435 to Dondeti et al. ("Dondeti") is entitled "Dual Encyrption Protocol for Scalable Secure Group Communication." Dondeti is directed to "[a] logical tree structure and method for managing membership in a multicast group." [Dondeti, at Abstract.] The protocol relied upon in Dondeti "requires that all . . . members obtain a capability certificate from designated certification authorities.] [Dondeti, at column 3, lines 17-19.]

U.S. Patent No. 6,772,331 to Hind ("Hind") is entitled "Method and Apparatus for Exclusively Pairing Wireless Devices." Hind is directed to "[a] method and system for enabling wireless devices to be paired or permanently associated by a user or a network administrator." [Hind, at Abstract.] In order to perform such a pairing, Hind uses an "administration server" or "initializing device" 1001 to pair with a device. [*See*, Hind, at column 9, lines 16-61; Figures 1A-1C.] *Hind also requires that the administration server request and receive trusted certificates from a separate Certificate Authority.*

> *At 1055 the administration server 1001 establishes a secure connection to a Certificate Authority 1005 and sends 1060 the certificate request 1050 that was prepared for mobile device 1003 to the Certificate authority whereupon the Certificate Authority 1005 signs 1065 and returns 1070 the certificate signed with the Certificate Authority's private key.* When the administration server 1001 receives the signed certificate 1050', it stores the certificate 1050' at step 1075 and sends the signed certificate 1050' and the corresponding private key (if the administration server generated the public/privae key pair) to the mobile device 1003 over the secure connection 1080 and sends the Certificate Authority's certificate (containing the CA's public key) to mobile device 1003 as well, and the session is ended.

[Hind, at column 9, lines 37-51; emphasis added.] Elsewhere, Hind describes the necessity of trust provided by third-party certificate authorities to its certificates:

> The exemplary certificate described contains the device's unique 48-bit IEEE (MAC) address (although any unique identifier could be used equally effectively), the device's public key, a validity period, and a signature from a Certificate Authority. . . . *The device must also acquire the root Certificate Authority's public key or the public*

key of a Certificate Authority in the chain authorization chain (herein after referred to as the CA's public key) so that it can verify the authenticity of certificates received from other devices. The signature of the Certificate Authority indicates that the association between device identifier and the public key in the device certificate can be trusted if the Certificate Authority is known and trusted. The public key of the Certificate Authority is used to verify its signature of other device certificates.

[Hind, at column 7, line 61 to column 8, line 13; emphasis added.]

Amendments

Editorial amendments have been made to claims 1, 2, and 13, and 19. No new matter is added.

Claims 1-20 Should be Allowable

The Action rejects claims 1-20 under 35 U.S.C. § 103(a) as being unpatentable over Hind in view of Dondeti. Applicants respectfully submit the claims in their present form are allowable over the cited art. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. (MPEP § 2142.)

The Action fails to make a establish a *prima facie* case of obviousness. Accordingly, applicants request that all rejections be withdrawn.

Claim 2

Claim 2, as amended, recites, in part:

generating a branding certificate at the branding device, the branding certificate instructing that the security-uninitialized device trust the branding device, the branding certificate further containing key data for verifying certificates provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device;

transmitting the branding certificate from the branding device to the security-uninitialized device via the secured network medium;

generating a trust group membership certificate at the branding device which is signed by the branding device, the trust group membership certificate containing a signed group name as well as a signed key identifying the security-uninitialized device

. . .

> *transmitting the trust group membership certificate from the branding device to the security-uninitialized device* via the secured network medium . . . .

[Emphasis added.] For example, the Application, describes the generation of branding certificates and trust group certificates by a branding device which is trusted by other devices:

> *The branding device 210 then generates a branding certificate 217 (Figure 2) at 410 that tells the networked computing device 220 to trust the branding device.* The branding certificate also provides the networked computing device with the branding device's public key for use in checking certificates provided by other devices that claim to be authorized by the branding device.
>
> *The branding device 210 also generates any other certificates the device needs in order to interact on the network at 412. These include trust group membership certificate(s) 216 (Figure 2) that identify the networked computing device to be a member of a trust group* (e.g., groups 140-142 in Figure 1). . . . *If the certificate is signed by the branding device, whom everyone has been programmed to trust, then the group membership certificate will be considered valid and the communication will be allowed.*
>
> At 414, the networked computing device 220 receives and stores the trust set-up information conveyed via the limited access network interface 222 from the branding device 210 into a trust set-up store 232.

[Application, at page 8, line 28 to page 9, line 15; *see also* Figure 4; emphasis added.] For at least the following reasons, Hind nor Dondeti, neither alone nor in combination, teach or suggest the above-quoted language of claim 2.

Hind's cannot teach or suggest a "branding device" which generates and transmits a "branding certificate" and a "trust group certificate" because Hind requires that certificates be requested and obtained from a third party certificate authority which otherwise is not party to Hind's pairing process.

In the rejection of the "branding certificate" language of claim 2, the Action cites to column 9, lines 15-60 of Hind. [Action, at § 7, p. 4.] In this passage, Hind describes the creation and transmission of public and private keys, as well as a device certificate to create trust between devices. While Applicants do not necessarily agree that Hind's "device certificate" reads on the "branding certificate" language of claim 2, Applicants note that, as discussed above, Hind utilizes a separate Certificate Authority, which does not communicate with the device, to create the device certificate:

> At 1055 the administration server 1001 establishes a secure connection to a Certificate Authority 1005 and sends 1060 the certificate request 1050 that was prepared for mobile device 1003 to the Certificate authority whereupon the Certificate Authority 1005 signs 1065 and returns 1070 the certificate signed with the Certificate

> Authority's private key. When the administration server 1001 receives the signed certificate 1050', it stores the certificate 1050' at step 1075 and sends the signed certificate 1050' and the corresponding private key (if the administration server generated the public/privae key pair) to the mobile device 1003 over the secure connection 1080 and sends the Certificate Authority's certificate (containing the CA's public key) to mobile device 1003 as well, and the session is ended.

[Hind, at column 9, lines 37-51.] Thus, while communication with and initialization of the device is performed by the administration server, it is this third-party Certificate Authority which creates the certificate and which is trusted sufficiently to perform this creating.

The Action also cites to column 10, lines 18-29 in rejection of the "trust group certificate" language of claim 2. [Action, at § 7, p. 5.] While Applicants do not necessarily agree that this passage describes a "trust group certificate" for a "group of devices," Applicants note that this passage describes two methods of sharing "group" information. In the first, Hind describes "associat[ing] the device with a particular user or group of users, the user or user group or device with access control groups," but only "[o]nce a public key, private key and certificate have been created." [Hind, at column 10, lines 18-23.] As such, this language cannot read on a "trust group membership *certificate*" as recited in claim 2.

As for Hind's second method of sharing information, Hind makes clear that, if any "group" information is included in a certificate, this information would simply be included in the same "device certificate" discussed above:

> *Yet another variation on the above embodiment is to include additional data in extension fields within the signed certificate.* Such additional fields could include, for example, user group associations, access control groups, etc. which then could be used in isolated pairing situations to allow autonomous access policy decisions to be made.

[Hind, at column 10, lines 24-29.] By being a part of the Hind's "device certificate," this information also cannot read on the above-quoted language of claim 2, as the certificate is requested of and created by the third-party Certificate Authority, as discussed above. For at least these reasons, Hind neither teaches nor suggests all limitations of claim 2. Applicants similarly do not find such disclosure in Dondeti, which as Applicants noted above, relies on "certification authorities" to provide trust.

As such, Hind and Dondeti, both taken separately and in combination, fail to teach or suggest all limitations of claim 2. The combination of Hind and Dondeti thus fails to demonstrate a *prima facie* case for the obviousness of claim 2. Claim 2, as well as its dependent claims 3-12, are allowable. Applicants request that the rejection of claims 2-12 be withdrawn and that the claims be allowed.

Claim 1

Claim 1, as amended, recites, in part:

> *generating group membership and cryptographic key data at the branding device*, the cryptographic key data for verifying group membership information provided by other devices on the open multi-access network to the security-uninitialized device are authenticated by the branding device
>
> *electronically imprinting the security-uninitialized device with the group membership and cryptographic key data by transmitting the group membership and cryptographic key data from the branding device to the security-uninitialized device via the secured network medium*; . . .

[emphasis added]. In its rejection of claim 1, the Action cites to similar sections of Hind and Dondeti as it cited to in its rejection of claim 2. For at least this reason, as well as the reasons cited above with respect to claim 2, Hind and Dondeti, taken alone or in combination, fail to state a *prima facie* case of obviousness. Thus, Claim 1, as well as its dependent claim 19, are allowable. Applicants request that the rejection of claims 1 and 19 be withdrawn and that the claims be allowed.

Claim 13

Claim 13, as amended, recites, in part:

> a security initializer operational to receive the branding public key from a branding device securely networked to the networked computing device, the branding device having previously generated the branding public key and trust group membership certificates, and further operational to initialize the security resolver with the branding public key.

[emphasis added]. In its rejection of claim 13, the Action cites only to the sections cited to in its rejection of claim 2. Tthe Action does not address specific language of claim 13 in its rejection. For at least this reason, as well as the reasons cited above with respect to claim 2, the Action does not demonstrate a *prima facie* case of obviousness over the combination of Hind and Dondeti for claim 13. Claim 13, as well as its dependent claims 14-18 and 20, are allowable. Applicants request that the rejection of claims 13-18 and 20 be withdrawn and that claims 13-18 and 20 be allowed.

Request for Interview

In view of the preceding amendments and remarks, Applicants believe the application to be allowable. If any issues remain, however, the Examiner is formally requested to contact the

undersigned attorney at (503) 226-7391 prior to issuance of the next communication in order to arrange a telephonic interview. This request is being submitted under MPEP § 713.01, which indicates that an interview may be arranged in advance by a written request.

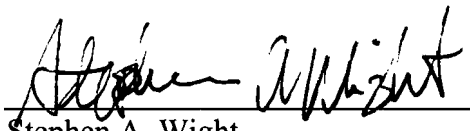
Conclusion

Claims 1-20 should be allowable. Such action is respectfully requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 595-5301

By 
Stephen A. Wight
Registration No. 37,759